JOURNAL OF ALGEBRA 5, 110-132 (1967)

New Results on Associative Division Algebras*

A. A. ALBERT

Department of Mathematics, The University of Chicago, Chicago, Illinois

Communicated by J. M. Herstein

Received March 6, 1966

1. INTRODUCTION

It is well known that every central division algebra of degree two or three is a cyclic algebra, and that every algebra of degree four is a crossed product. It is also known that there exist noncyclic algebras of degree four. Very little is known about algebras of degree $n > 4$.

The principal question in the theory of associative division algebras is then the question of the existence of algebras which are not crossed products. It is thus natural to discuss algebras of prime degree p, a case where every crossed product is cyclic.

We shall address ourselves here to a study of the nature of division algebras $\mathfrak{D}$ of prime degree p over a field $\mathfrak{F}$ of characteristic p, and shall limit our discussion to the case where *there exists a quadratic extension* $\mathfrak{K}$ *of* $\mathfrak{F}$ *such that the extension* $\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{K}$ *is a cyclic algebra*. We are thus studying cyclic algebras $\mathfrak{D}_0 = \mathfrak{H} + \mathfrak{H}y_S + \cdots + \mathfrak{H}y_S^{p-1}$, where $\mathfrak{H}$ is the cyclic field such that $\mathfrak{H} = \mathfrak{K}(x)$ for $x^p - x = a$ in $\mathfrak{K}$, and $y_S x = (x + 1)y$, $y_S{}^p = g$ in $\mathfrak{K}$. If $\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{K}$ then it is easy to see that $\mathfrak{D}$ is cyclic if either $\mathfrak{H}$ is normal over $\mathfrak{K}$ or if the field $\mathfrak{K}' = \mathfrak{K}(g^{1/p}, \bar{g}^{1/p})$ does not have degree p^2 over $\mathfrak{K}$. We consider the case where $\mathfrak{H}$ *is not normal* and $\mathfrak{K}'$ does have degree p^2 over $\mathfrak{K}$, so that $\mathfrak{K}'$ is isomorphic over $\mathfrak{K}$ to the polynomial ring $\mathfrak{K}_0 = \mathfrak{K}[y, y']$, where $y^p = g\bar{g}$ and $y'^p = (g(\bar{g})^{-1}$. Define the derivations D and D' of $\mathfrak{K}_0$ by $(\alpha y^i y'^j)D = \alpha i y^i y'^j$, and $(\alpha y^i y'^j)\mathfrak{D}' = \alpha y^i j y'^j$ for α in $\mathfrak{K}$. We also define a conjugate operation $\phi \to \phi^*$ of $\mathfrak{K}_0$ by $(\alpha y^i y'^j)^* = \bar{\alpha} y^i (y')^{-j}$ for α in $\mathfrak{K}$. Then we shall show that $\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{K}$ for a central division algebra $\mathfrak{D}$ over $\mathfrak{F}$ if and only if there exists a canonical generator x of $\mathfrak{H}$ over $\mathfrak{K}$ such that $x^p - x = a = (\theta + \theta')^p$ for $\theta = \sum_{i=1}^{p-1} \sum_{j=0}^{p-1} \theta_{ij} y^i y'^j$ and $\theta' = \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} \theta'_{ij} y^i (y')^j$, where $\theta D' = \theta' D$, $\theta^* = -\theta$, $\theta'^* = \theta'$. These last conditions are consistent and define a wide class of algebras which may contain noncyclic algebras. A machinery for

* The research of this paper was supported, in part, by a National Science Foundation grant.

testing one of these algebras for cyclicity is given and some of the steps in the applications of this machinery are taken. However, the computations required are still being studied and it may be some time before the cyclicity of even the special case given here is determined for the simplest case, where $p = 5$.

2. A Non-Abelian Normal Field

Let $\mathfrak{F}$ be an arbitrary field of characteristic p, ρ be a nonsquare element of $\mathfrak{F}$, $u^2 = \rho$ so that $\mathfrak{K} = \mathfrak{F}(u)$ is a quadratic extension of $\mathfrak{F}$. Then $\mathfrak{K}$ has an automorphism of period two over $\mathfrak{F}$ called its *conjugate* operation and defined by

$$b = \gamma + \delta u \to \bar{b} = \gamma - \delta u \qquad (\gamma, \delta \text{ in } \mathfrak{F}). \tag{1}$$

We now consider a cyclic field $\mathfrak{H}$ of degree p over $\mathfrak{K}$. It is well known that every such $\mathfrak{H}$ has a *canonical generator x such that*

$$x^p = x + a, \tag{2}$$

where a is in $\mathfrak{K}$. Then the automorphism group of $\mathfrak{H}$ over $\mathfrak{K}$ is generated by an automorphism S such that $xS = x + 1$. Moreover, every canonical generator of $\mathfrak{H}$ over $\mathfrak{K}$ has the form $x' = k(x + \lambda)$ for a nonzero *integer* k and for λ in $\mathfrak{K}$, where then $x'^p = k^p(x^p + \lambda^p) = k(x + a + \lambda^p) = k(x + \lambda + a + \lambda^p - \lambda)$. Thus every canonical generator of $\mathfrak{H}$ satisfies an equation of the form $(x')^p = x' + a'$ with

$$a' = k(a + \lambda^p - \lambda). \tag{3}$$

We now proceed to discuss the possible structure of $\mathfrak{H}$ over the field $\mathfrak{F}$. It is, of course, possible that $\mathfrak{H} = \mathfrak{H}_0 \times \mathfrak{K}$ where $\mathfrak{H}_0 = \mathfrak{F}(x)$ is cyclic of degree p over $\mathfrak{F}$. This occurs if and only if $\mathfrak{H}$ has a canonical generator x' such that the corresponding element a' is in $\mathfrak{F}$. When $\mathfrak{H}$ does not have that structure, $\mathfrak{H}$ can still be normal but not cyclic over $\mathfrak{F}$. In this second case $\mathfrak{H}$ has a canonical generator with $\bar{a}' = -a'$. *We shall assume henceforth that $\mathfrak{H}$ is not normal over $\mathfrak{F}$*, and thus that $\mathfrak{H}$ *has no canonical generator x* such that $a = \bar{a}$ or $a = -\bar{a}$. It is evident that this needs to be verified only for the value $k = 1$ in our formula (3).

Let us embed $\mathfrak{H}$ in a normal field

$$\mathfrak{L} = \mathfrak{H}(\bar{x}) = \mathfrak{K}(x, \bar{x}) = \mathfrak{F}(x, \bar{x}) \tag{4}$$

of degree $2p^2$ over $\mathfrak{F}$ and consequently of degree p^2 over $\mathfrak{K}$. Then $\mathfrak{L}$ is the direct product

$$\mathfrak{L} = \mathfrak{H} \times \bar{\mathfrak{H}}, \qquad \bar{\mathfrak{H}} = \mathfrak{K}(\bar{x}), \qquad \bar{x}^p - \bar{x} = \bar{a}, \qquad \bar{x}T = \bar{x} + 1. \tag{5}$$

The field $\bar{\mathfrak{H}}$ is cyclic of degree p over $\mathfrak{K}$, T is an automorphism of $\mathfrak{L}$ over $\mathfrak{F}$ inducing the generating automorphism $\bar{h} \to \bar{h}T$ of $\bar{\mathfrak{H}}$ over $\mathfrak{K}$, and $\mathfrak{H}$ is actually the fixed field of $\mathfrak{L}$ under T.

The normal field $\mathfrak{L}$ over $\mathfrak{F}$ is the root field of the separable polynomial

$$f(\lambda) = (\lambda^p - \lambda - a)(\lambda^p - \lambda - \bar{a}), \tag{6}$$

a polynomial of degree $2p$ with coefficients in $\mathfrak{F}$ and roots $x + i$, $\bar{x} + j$ for $i, j = 0, 1, \ldots, p - 1$. The automorphism group $\mathfrak{G}$, of $\mathfrak{L}$ over $\mathfrak{F}$, is generated by three automorphisms S, T, and J over $\mathfrak{F}$. These automorphisms are induced by the relations

$$\begin{aligned} &xS = x + 1, \quad \bar{x}S = \bar{x}, \qquad uS = u, \quad \bar{x}T = \bar{x} + 1, \quad xT = x, \\ &uT = u, \qquad uJ = -u, \quad xJ = \bar{x}, \quad \bar{x}J = x. \end{aligned} \tag{7}$$

Then a set of defining relations for $\mathfrak{G}$ are the relations

$$S^p = T^p = J^2 = I, \qquad ST = TS, \qquad JT = SJ. \tag{8}$$

Evidently $(SJ)^2 = ST$, and so $\mathfrak{G}$ is generated by S and J.

We now define two subfields of $\mathfrak{L}$. The first is the field

$$\mathfrak{F} = \mathfrak{F}(z), \qquad z = \tfrac{1}{2}(x + \bar{x}), \qquad z^p = z + \tfrac{1}{2}(a + \bar{a}). \tag{9}$$

This field is cyclic of degree p over $\mathfrak{F}$. Indeed, if

$$U = ST, \qquad V = ST^{-1}, \tag{10}$$

then $\mathfrak{F}$ is the fixed field of $\mathfrak{L}$ under the subgroup of $\mathfrak{G}$ generated by V and J. For clearly

$$JU = UJ, \qquad JV = V^{-1}J \tag{11}$$

and $zV = zJ = z$. The group generated by J and V is a normal subgroup of $\mathfrak{G}$ since $\mathfrak{G}$ is generated by U, V and J, and $UVU^{-1} = V$, $UJU^{-1} = J$. But $zU = z + 1$, so that z is not in $\mathfrak{F}$, and thus the field $\mathfrak{F}$, of degree p over $\mathfrak{F}$, is $\mathfrak{F}(z)$.

We also define a subfield

$$\mathfrak{W} = \mathfrak{F}(w) = \mathfrak{K}(w), \qquad w = \tfrac{1}{2}(x - \bar{x}), \tag{12}$$

so that

$$w^p = w + \tfrac{1}{2}(a - \bar{a}), \qquad wU = w, \qquad wJ = -w, \qquad wV = w + 1. \tag{13}$$

This field is cyclic of degree p over $\mathfrak{K}$, but is *not cyclic* over $\mathfrak{F}$.

We now pass to the study of a certain class of associative division algebras of degree p over $\mathfrak{F}$ of characteristic p.

3. Division Algebras of Prime Degree

Consider a division algebra $\mathfrak{D}$ of prime degree p over its center $\mathfrak{F}$ of characteristic p. We make the *fundamental assumption* that there exists a *quadratic* extension $\mathfrak{K}$ of $\mathfrak{F}$ such that *the scalar extension*

$$\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{K} = \mathfrak{D}_{\mathfrak{K}} \tag{14}$$

is *cyclic* over $\mathfrak{K}$. Then $\mathfrak{D}_0$ must contain a subfield $\mathfrak{H} = \mathfrak{F}(x) = \mathfrak{K}(x)$ defined as in (2). If $\mathfrak{H}$ is the cyclic field $\mathfrak{H}_1 \times \mathfrak{K}$, where H_1 is cyclic over F, the algebra $\mathfrak{D}$ is trivially a cyclic algebra over $\mathfrak{F}$. For $\mathfrak{H}_1$ must split $\mathfrak{D}$. If $\mathfrak{H}$ is normal but not cyclic over $\mathfrak{F}$ then we have shown elsewhere[1] that $\mathfrak{D}$ is cyclic over $\mathfrak{F}$. We shall therefore assume henceforth that $\mathfrak{H}$ is not normal over $\mathfrak{F}$. Then we shall embed $\mathfrak{H}$ in the normal field $\mathfrak{L}$ over $\mathfrak{F}$ with the properties described in Section 2. Let us repeat that our assumption on $\mathfrak{H}$ is equivalent to the hypothesis that the function

$$a(\alpha) = a + \alpha^p - \alpha \neq \overline{a(\alpha)}, \quad \overline{a(\alpha)}, \tag{15}$$

for any α of $\mathfrak{K}$. This latter condition is easily seen to be equivalent to the irreducibility over $\mathfrak{K}$ of each of the polynomials $\lambda^p - \lambda - (a + \bar{a})$ and $\lambda^p - \lambda - (a - \bar{a})$.

We shall now observe some consequences of our definitions and shall introduce some notations. We observe first that $\mathfrak{D}_{\mathfrak{K}}$ is the cyclic algebra

$$\mathfrak{D}_0 = \mathfrak{D}_{\mathfrak{K}} = (\mathfrak{H}, S, g) = (\mathfrak{H}, y_S, g) = \mathfrak{H} + \mathfrak{H}y_S + \cdots + \mathfrak{H}y_S^{p-1}, \tag{16}$$

defined by the relations

$$y_S x = (x + 1)y_S, \qquad y_S{}^p = g \qquad (g \neq 0 \text{ in } \mathfrak{K}), \tag{17}$$

where we will find it convenient to use the new notation $(\mathfrak{H}, y_S, g)$ to indicate the element y_S of (17). As is well known, $\mathfrak{D}_0$ is a divsion algebra if and only if $g \neq N_S(h)$ for any h in $\mathfrak{K}$, where the norm $N_S(h)$ is defined by

$$N_S(h) = h(hS) \cdots (hS^{p-1}). \tag{18}$$

The algebra $\mathfrak{D} \times \mathfrak{K} = \mathfrak{D}_{\mathfrak{K}}$ is a subalgebra of the direct product

$$\mathfrak{D} \times \mathfrak{M}_2, \tag{19}$$

where $\mathfrak{M}_2$ is the full matric algebra of degree two over $\mathfrak{F}$ and we may write

$$\mathfrak{M}_2 = \mathfrak{K} + \mathfrak{K}v, \qquad vu = -uv, \qquad v^2 = 1. \tag{20}$$

[1] See the author's On associative division algebras of prime degree. *Proc. Am. Math. Soc.* **16** (1965), 799-802.

Then

$$\begin{aligned} vy_Sv^{-1} &= y_T', y_T'(vxv^{-1}) = v(y_Sx)v^{-1} = v[(x+1)y_S]v^{-1} \\ &= (vxv^{-1}+1)y_T', y_T'^p = (vy_Sv^{-1})^p = vgv^{-1} = \bar{g}. \end{aligned} \tag{21}$$

It follows that $\mathfrak{D} \times \mathfrak{K} = \mathfrak{D}_{\mathfrak{K}}$ is *isomorphic* over $\mathfrak{K}$ to the algebra

$$(\bar{\mathfrak{H}}, T, \bar{g}) = (\bar{\mathfrak{H}}, y_T, \bar{g}) = \bar{\mathfrak{H}} + \bar{\mathfrak{H}}y_T + \cdots + \bar{\mathfrak{H}}y_T^{p-1}, \tag{23}$$

in which $\bar{\mathfrak{H}} = \mathfrak{K}(\bar{x})$ is isomorphic over $\mathfrak{K}$ to $\mathfrak{K}(vxv^{-1})$, and

$$\bar{x}^p = \bar{x} + \bar{a}, \qquad y_T\bar{x} = (\bar{x}+1)y_T, \qquad y_T{}^p = \bar{g}. \tag{24}$$

Observe that the element y_T in (23) and (24) is *not* the element $vy_Sv^{-1} = y_T'$ of the algebra $\mathfrak{D}_{\mathfrak{K}}$, and part of our problem is that *we are unable to write explicit formulas for* vxv^{-1} *and* vy_Sv^{-1}.

We now begin a study of the algebra

$$\mathfrak{A} = \mathfrak{D} \times \mathfrak{D} \times \mathfrak{M}_2 = \mathfrak{D}^2 \times \mathfrak{M}_p \times \mathfrak{M}_2, \tag{25}$$

where we are using the notation $\mathfrak{M}_t$ for the t-rowed full matrix algebra (over $\mathfrak{F}$). It is, of course, well known that

$$\mathfrak{D} \times \mathfrak{D} = \mathfrak{D}^2 \times \mathfrak{M}_p, \tag{26}$$

for a central division algebra $\mathfrak{D}^2$ of degree p over $\mathfrak{F}$. This algebra contains the subalgebra

$$\mathfrak{B} = \mathfrak{D} \times \mathfrak{D} \times \mathfrak{K} = \mathfrak{D}_{\mathfrak{K}} \times \mathfrak{D}_{\mathfrak{K}} = (\mathfrak{H}, y_S, g) \times (\bar{\mathfrak{H}}, y_T, \bar{g}), \tag{27}$$

over $\mathfrak{K}$, where (22)–(24), (16), and (17) all hold and the condition

$$\bar{g} \neq N_T(\bar{h}) = \bar{h}(\bar{h}T) \cdots (\bar{h}T^{p-1}) \tag{28}$$

holds for any $\bar{h}$ of $\bar{\mathfrak{H}}$. The center of $\mathfrak{B}$ is clearly $\mathfrak{K}$, and the theory of cyclic algebras implies that

$$\mathfrak{D}_{\mathfrak{K}} \times \mathfrak{D}_{\mathfrak{K}} = (\bar{\mathfrak{H}}_0, y_{0S}, g^2) \times (\bar{\mathfrak{H}}_0, y_{0T}, 1), \tag{29}$$

where $(\bar{\mathfrak{H}}_0, y_{0T}, 1)$ is isomorphic over $\mathfrak{K}$ to $\mathfrak{M}_p$, $\mathfrak{H}_0$ is isomorphic over $\mathfrak{K}$ to $\mathfrak{H}$, $\bar{\mathfrak{H}}_0$ is isomorphic over $\mathfrak{K}$ to $\bar{\mathfrak{H}}$. Thus

$$\mathfrak{D}_{\mathfrak{K}}{}^2 \cong (\mathfrak{H}_0, y_{0S}, g^2). \tag{30}$$

However, every automorphism over $\mathfrak{K}$ of two simple subalgebras of a central simple algebra $\mathfrak{B}$ over $\mathfrak{K}$ can be extended to an inner automorphism over $\mathfrak{K}$

of $\mathfrak{B}$. Since $\mathfrak{H}_0$ is isomorphic over $\mathfrak{K}$ to $\mathfrak{H}$, and $\bar{\mathfrak{H}}_0$ is isomorphic over $\mathfrak{K}$ to $\bar{\mathfrak{H}}$, the direct product $\mathfrak{H}_0 \times \bar{\mathfrak{H}}_0$ is isomorphic over $\mathfrak{K}$ to $\mathfrak{L} = \mathfrak{H} \times \bar{\mathfrak{H}}$. Thus we can take $\mathfrak{H}_0 = \mathfrak{H}$, $\bar{\mathfrak{H}}_0 = \bar{\mathfrak{H}}$ and we have derived a result which we state as follows.

LEMMA 1. *Let* $\mathfrak{B} = \mathfrak{D} \times \mathfrak{D} \times \mathfrak{K}$ *so that, since* $\mathfrak{D}_{\mathfrak{K}} = (\mathfrak{H}, S, g)$ *and* $(\bar{\mathfrak{H}}, T, \bar{g})$ *are isomorphic over* $\mathfrak{K}$, *we can take*

$$\mathfrak{B} = (\mathfrak{H}, y_S, g) \times (\bar{\mathfrak{H}}, y_T, \bar{g}). \tag{31}$$

Then

$$\mathfrak{B} = (\mathfrak{H}, y_S{}^*, g^2) \times (\bar{\mathfrak{H}}, y_T{}^*, 1), \tag{32}$$

for the same field $\mathfrak{L} = \mathfrak{H} \times \bar{\mathfrak{H}}$ *in* (31) *and* (32).

The result of Lemma 1 implies some properties of norms of certain elements in $\mathfrak{L}$. However, these results do not seem to lead to the main result of this paper and will not be given here.

4. EXPRESSION OF $\mathfrak{A}$ AS A CROSSED PRODUCT

The algebra $\mathfrak{A} = \mathfrak{D} \times \mathfrak{M}_p \times \mathfrak{M}_2$ is a central simple algebra of degree $2p^2$ over $\mathfrak{F}$ and it contains $\mathfrak{B} = (\mathfrak{H}, y_S, g) \times (\bar{\mathfrak{H}}, y_T, \bar{g})$. Thus $\mathfrak{L}$ is a maximal normal subfield of $\mathfrak{A}$, and so $\mathfrak{A}$ is a *crossed product over* $\mathfrak{F}$. Then

$$\mathfrak{A} = \mathfrak{B} + \mathfrak{B}v, \tag{33}$$

where (20) holds. We now propose to complete the details of the expression of $\mathfrak{A}$ as a crossed product.

Define an algebra

$$\mathfrak{A}_0 = \mathfrak{B} + \mathfrak{B}y_J, \tag{34}$$

where

$$y_J x = \bar{x} y_J, \qquad y_J y_S = y_T y_J, \qquad y_J{}^2 = 1, \tag{35}$$

for the elements y_S and y_T of $\mathfrak{B} = (\mathfrak{H}, y_S, g) \times (\bar{\mathfrak{H}}, y_T, \bar{g})$, where $\mathfrak{H} = \mathfrak{K}(x)$ and $\bar{\mathfrak{H}} = \mathfrak{K}(\bar{x})$. The elements of $\mathfrak{B}$ are all finite sums of products MM' of elements $M = \sum_{i=0}^{p-1} h_i y_S{}^i$ of $(\mathfrak{H}, y_S, g)$ and elements $M' = \sum_{j=0}^{p-1} \bar{h}_j' y_T{}^j$ of $(\bar{\mathfrak{H}}, y_T, \bar{g})$. The mappings

$$M \to MJ = \sum_{i=0}^{p-1} (h_i J) y_T{}^i, \qquad M' \to M'J = \sum_{j=0}^{p-1} h_j' y_S{}^j, \tag{36}$$

defined by $h_j' = \bar{h}_j' J$, induces the automorphism J over $\mathfrak{F}$ of $\mathfrak{B}$ which is defined by

$$\left[\sum_{i=1}^{t} M_i M_i'\right] J = \sum_{i=1}^{t} (M_i J)(M_i' J). \tag{37}$$

This automorphism evidently induces the automorphism J over $\mathfrak{F}$ of the field $\mathfrak{L}$. It should also be obvious, from (37), that if N is any element of B, then $NJ^2 = N$, so that J^2 is the identity automorphism of $\mathfrak{B}$ over $\mathfrak{F}$.

We now define products in $\mathfrak{A}_0$ by

$$(N_1 + N_2 y_J)(N_3 + N_4 y_J) = [N_1 N_3 + N_2(N_4 J)] + [N_1 N_4 + N_2(N_3 J)] y_J, \tag{38}$$

for all N_1, N_2, N_3, N_4 in $\mathfrak{B}$, and see that $\mathfrak{A}_0$ is an algebra over $\mathfrak{F}$ and contains $\mathfrak{B}$. It is trivial to verify that $\mathfrak{A}_0$ is associative and has dimension $2p^2$ over $\mathfrak{F}$. But $\mathfrak{A}_0$ contains $\mathfrak{B} = \mathfrak{D} \times \mathfrak{M}_p \times \mathfrak{K}$, and so $\mathfrak{A}_0 = \mathfrak{D} \times \mathfrak{M}_p \times \mathfrak{Q}$ where $\mathfrak{Q}$ is a quaternion algebra. Evidently the subalgebra $\mathfrak{K} + \mathfrak{K} y_J$ of $\mathfrak{A}_0$ is isomorphic over $\mathfrak{F}$ to $\mathfrak{M}_2$, and so $\mathfrak{Q}$ must split, $\mathfrak{Q}$ is isomorphic to $\mathfrak{M}_2$. Thus $\mathfrak{A}_0 = \mathfrak{D} \times \mathfrak{M}_p \times \mathfrak{M}_2$ is isomorphic to $\mathfrak{A}$, and our proof is complete. We state this result as follows.

THEOREM 1. *Let* $\mathfrak{A} = \mathfrak{B} + \mathfrak{B} y_J$, *where* $\mathfrak{B} = (\mathfrak{H}, y_S, g) \times (\bar{\mathfrak{H}}, y_T, \bar{g})$ *and* $y_J^2 = 1$, $y_J y_S = y_T y_J$, $y_J x = \bar{x} y_J$. *Then* $\mathfrak{A}$ *is a crossed product over* $\mathfrak{F}$ *with* $\mathfrak{L}$ *as maximal subfield,* $\mathfrak{A} = \mathfrak{D} \times \mathfrak{M}_p \times \mathfrak{M}_2$.

We observe that the problem of *extracting* the factor $\mathfrak{D}$ of $\mathfrak{A}$ is quite another and exceedingly difficult problem. We shall pass on now to consider a property of p-algebras.

5. A PROPERTY OF p-ALGEBRAS OF DEGREE p

Consider a cyclic algebra $\mathfrak{E}$ of degree p over a field $\mathfrak{K}$. We have seen that we can write

$$\mathfrak{E} = (\mathfrak{C}, y, \gamma) = \mathfrak{C} + \mathfrak{C} y + \cdots + \mathfrak{C} y^{p-1}, \tag{39}$$

where $\mathfrak{C} = \mathfrak{K}(c)$ for a canonical generator c such that

$$c^p = c + \alpha, \qquad yc = (c + 1)y, \qquad y^p = \gamma, \tag{40}$$

for α and $\gamma \neq 0$ in $\mathfrak{K}$. The arbitrary element of $\mathfrak{E}$ has the form $f = \sum_{i=0}^{p-1} f_i y^i$ for f_i in $\mathfrak{C}$, and $fy - yf = \sum (f_i - f_i S) y^i = 0$ if and only if every $f_i = f_i S$, every f_i is in $\mathfrak{K}$, f is in the ring $\mathfrak{K}[y]$.

Let us now suppose that c_1 is in $\mathfrak{E}$ and is such that $yc_1 = (c_1 + 1)y$. Then $yc_1^p y^{-1} = c_1^p + 1$ and so $y(c_1^p - c_1)y^{-1} = c_1^p - c_1$. Thus $c_1^p - c_1$ is in $\mathfrak{R}[c_1]$ and in $\mathfrak{R}[y]$. The intersection of these two commutative subalgebras of dimension p over $\mathfrak{R}$ is $\mathfrak{R}$, and c_1 generates a separable algebra which is either a cyclic field with c_1 as canonical generator or has a canonical generator c_2 such that $c_2^p = c_2$. We seek to find the elements c_1 and the elements $\alpha_1 = c_1^p - c_1$.

We first see that, if $ycy^{-1} = c + 1$, and $yc_1y^{-1} = c_1 + 1$ then $y(c - c_1)y^{-1} = c - c_1$. Thus $c_1 - c$ is in $\mathfrak{R}[y]$, and we may write

$$c_1 = c - \phi, \qquad \phi = \phi(y) = \phi_0 + \phi_1 y + \cdots + \phi_{p-1}y^{p-1} \qquad (\phi_i \text{ in } K). \tag{41}$$

Then (40) implies that

$$\phi c = c\phi + \phi D, \tag{42}$$

where D is given by

$$\phi D = \phi_1 y + 2\phi_2 y^2 + \cdots + i\phi_i y^i + \cdots + (p-1)\phi_{p-1}y^{p-1}. \tag{43}$$

The mapping $\phi \to \phi D$ is then a *derivation of the polynomial ring* $\mathfrak{R}[y]$, such that $yD = y$. We define D^μ, for every integer μ, by the inductive formula $\phi D^{\mu+1} = (\phi D^\mu)D$, and see that

$$\phi D^p = \phi D, \quad \phi D^{p-1} = \sum_{i=1}^{p-1} \phi_i i^{p-1} y^i = \phi - \phi_0. \tag{44}$$

Nathan Jacobson[2] has derived the following result. Write $c_1 = c - \phi$ as in (41) for any ϕ in $\mathfrak{R}[y]$. Then it has been shown that

$$c_1^p = c^p - V_p(\phi), \tag{45}$$

where

$$V_p(\phi) = \phi^p + \phi D^{p-1}. \tag{46}$$

But then $c_1^p = c + \alpha - (\phi^p + \phi D^{p-1})$, and we have the property

$$c_1^p = c_1 + \alpha_1, \qquad \alpha_1 = \alpha - (\phi^p - \phi_0). \tag{47}$$

Evidently $yc_1 = (c_1 + 1)y$ and it follows that

$$(\mathfrak{C}, y, \gamma) = (\mathfrak{C}_1, y, \gamma), \tag{48}$$

where $\mathfrak{C}_1 = \mathfrak{R}[c_1] = \mathfrak{R}[c - \phi]$ for every ϕ in $\mathfrak{R}[y]$.

[2] p-Algebras of exponent p. *Bull. Am. Math. Soc.* 43 (1937), 667-670.

When $\mathfrak{R}[y]$ is not a field the algebra $(\mathfrak{C}, y, \gamma)$ is a full matrix algebra. When $\mathfrak{R}[y] = \mathfrak{R}(y)$ is a field it is known that $(\mathfrak{C}, y, \gamma)$ is a full matrix algebra if and only if $(\mathfrak{C}, y, \gamma)$ is isomorphic to $(\mathfrak{C}_1, y, \gamma)$, where $\alpha_1 = 0$ in (47). We state this result as follows.

LEMMA 2. *Let $\mathfrak{R}(y)$ be a field. Then $(\mathfrak{C}, y, \gamma)$ is isomorphic to $(\mathfrak{C}_1, y, \gamma)$ for $\mathfrak{C}_1 = \mathfrak{R}[c_1]$ where $c_1 = c - \phi$, ϕ is any element of $\mathfrak{R}[y]$ and thus*

$$c_1^p - c_1 = \alpha_1 = \alpha - (\phi^p - \phi_0) = \alpha - \left[\sum_{i=1}^{p-1} \phi_i^p \gamma^i + (\phi_0^p - \phi_0)\right] \quad (49)$$

for $\phi_0, \ldots, \phi_{p-1}$ in $\mathfrak{R}$. Then $(\mathfrak{C}, y, \gamma)$ is a division algebra if and only if the equation $\alpha = \phi^p - \phi_0$ does not hold for any $\phi_0, \ldots, \phi_{p-1}$ in $\mathfrak{R}$.

The condition in (49) is clearly simpler than the general condition which states that $(\mathfrak{C}, y, \gamma)$ is a division algebra if and only if $y \neq N(c)$ for any k in $\mathfrak{C}$, as the norm form is considerably more complicated than the expression $\phi^p - \phi_0$ of (49).

6. APPLICATION OF THE JACOBSON FORMULA

We will now obtain the basic result of this paper. We consider the algebra

$$\mathfrak{D}_1 = (\mathfrak{H}, y, g\bar{g}) = \mathfrak{H} + \mathfrak{H}y + \cdots + \mathfrak{H}y^{p-1} \quad (50)$$

over $\mathfrak{R}$, where

$$\mathfrak{H} = \mathfrak{R}(x), \qquad x^p = x + a, \qquad yx = (x + 1), \qquad y^p = g\bar{g}, \quad (51)$$

for a and g in $\mathfrak{R}$. We also let

$$\mathfrak{H}' = \mathfrak{R}(x'), \qquad (x')^p = x' + a', \quad (52)$$

so that $\mathfrak{H}$ and $\mathfrak{H}'$ are isomorphic over $\mathfrak{R}$, and define an algebra

$$\mathfrak{D}_2 = (\mathfrak{H}', y', g/\bar{g}) = \mathfrak{H}' + \mathfrak{H}'y' + \cdots + \mathfrak{H}'(y')^{p-1}, \quad (53)$$

where

$$y'x' = (x' + 1)y', \qquad y'^p = g(\bar{g})^{-1}. \quad (54)$$

We then form the direct product

$$\mathfrak{B}_0 = \mathfrak{D}_1 \times \mathfrak{D}_2 . \quad (55)$$

By the theory of cyclic algebras we have

$$\mathfrak{B}_0 = (\mathfrak{H}_1, y, g\bar{g}) \times (\mathfrak{H}', y'g/\bar{g}) = (\mathfrak{H}, y'', g^2) \times (\mathfrak{H}', y''', 1). \tag{56}$$

Indeed $(\mathfrak{H}', y''', 1) = \mathfrak{M}_p \times \mathfrak{R}$ and so

$$\mathfrak{B}_0 = (\mathfrak{H}, y'', g^2) \times (\mathfrak{H}_0, y', g/\bar{g}), \tag{57}$$

where

$$\mathfrak{H}_0 = \mathfrak{R}[x - x'], \qquad (x - x')^p = x - x', \qquad y'' = yy', \tag{58}$$

and $(\mathfrak{H}_0, y', g/\bar{g})$ has already been seen to be a total matrix algebra. We thus see that, since $(\mathfrak{H}, y'', g^2) \cong \mathfrak{D}_K{}^2$, we have

$$\mathfrak{B}_0 = \mathfrak{D}_1 \times \mathfrak{D}_2 \cong \mathfrak{M}_p \times \mathfrak{D}_K{}^2 \cong \mathfrak{B}. \tag{59}$$

We may thus take $\mathfrak{B} = \mathfrak{B}_0$ and have shown that $\mathfrak{D}_1 \times \mathfrak{D}_2$ can be embedded in the algebra $\mathfrak{A} = \mathfrak{B} + \mathfrak{B}y_J$ of (34) and (35). Let us now define

$$y_J y y_J = y_1, \qquad y_J y' y_J = y_1', \qquad y_J x y_J = x_1, \qquad y_J x' y_J = x_1', \tag{60}$$

where

$$x_1{}^p = x_1 + \bar{a}, x_1'{}^p = x_1' + \bar{a}, y_1 x_1 = (x_1 + 1)y_1, y_1' x_1' = (x_1' + 1)y_1'. \tag{61}$$

We also know that

$$x_1 x_1' - x_1' x_1 = x_1 y_1' - y_1' x_1 = x_1' y_1 - y_1 x_1' = y_1 y_1' - y_1' y_1 = 0, \tag{62}$$

and that

$$y_1{}^p = g\bar{g}, y_1'{}^p = \bar{g}(g^{-1}). \tag{63}$$

We now have the following result.

LEMMA 3. *If the field* $\mathfrak{R}(g^{1/p}, \bar{g}^{1/p})$ *does not have degree* p^2 *over* $\mathfrak{R}$ *the algebra* $\mathfrak{D}$ *is cyclic over* F.

For $\mathfrak{D}$ is a division algebra and so $\mathfrak{R}(y)$ must be a field of degree p over $\mathfrak{R}$. Then $\mathfrak{R}_1 = \mathfrak{R}(g^{1/p})$ has degree p over $\mathfrak{R}$, and $\mathfrak{R}_1(\bar{g}^{1/p})$ either has degree p over $\mathfrak{R}_1$ or degree one over $\mathfrak{R}_1$. In the former case $\mathfrak{R}(g^{1/p}, \bar{g}^{1/p}) = \mathfrak{R}_1(g^{1/p})$ has degree p^2 over $\mathfrak{R}$. In the latter case $\bar{g}^{1/p}$ is in $\mathfrak{R}_1$, $\mathfrak{R}_1$ contains $(g\bar{g})^{1/p}$. If $(g\bar{g})^{1/p}$ is not in $\mathfrak{F}$ it is not in $\mathfrak{R}$ and so $\mathfrak{R}_1 \supseteq \mathfrak{R}((g\bar{g})^{1/p})$ which has degree p over $\mathfrak{R}$, $\mathfrak{R}_1 = \mathfrak{R}((g\bar{g})^{1/p})$. But then $g^{1/p}$ is in $\mathfrak{R}((g\bar{g})^{1/p})$, $\mathfrak{R}((g\bar{g})^{1/p})$ splits $\mathfrak{D}_\mathfrak{R}$, $\mathfrak{F}((g\bar{g})^{1/p})$ splits $\mathfrak{D}$, and so $\mathfrak{D}$ is cyclic over $\mathfrak{F}$. Otherwise $(g\bar{g})^{1/p} = \epsilon$ in $\mathfrak{F}$, $\bar{g} = \epsilon^p g^{-1}$, $g(\bar{g})^{-1} = \epsilon^{-p} g^2$, $\delta = g(\bar{g})^{-1} + \bar{g}g^{-1} = \epsilon^{-p}(g^2 + \bar{g}^2) = \epsilon^{-p} g^2 + \epsilon^p g^{-2}$ is in $\mathfrak{F}$,

$\delta^{1/p} = \epsilon^{-1}(\bar{g}^{1/p})^2 + \epsilon(g^{1/p})^{-2}$ is not in $\mathfrak{F}$, $\mathfrak{K}(\delta^{1/p})$ has degree p over $\mathfrak{K}$, $\mathfrak{K}(\delta^{1/p}) = \mathfrak{K}(g^{1/p})$ splits $\mathfrak{D}_{\mathfrak{K}}$, $\mathfrak{K}(\delta^{1/p})$ splits $\mathfrak{D}$, and $\mathfrak{D}$ is cyclic. This completes our proof.

As a consequence of Lemma 3 we have the follwing necessary condition.

LEMMA 4. *Suppose that $\mathfrak{D}$ is not cyclic. Then $\mathfrak{K}[y, y']$ is a field.*

For $\mathfrak{K}[y, y'] = \mathfrak{K}[yy', y(y')^{-1}]^p = \bar{g}^2$, and $\mathfrak{K}((g^2)^{1/p}, (\bar{g}^2)^{1/p}) = \mathfrak{K}(g^{1/p}, \bar{g}^{1/p})$ is a field of degree p^2 over $\mathfrak{K}$. Then the ring $\mathfrak{K}[y, y']$, of dimension p^2 over $\mathfrak{K}$, is isomorphic over $\mathfrak{K}$ to $\mathfrak{K}(g^{1/p}, \bar{g}^{1/p})$, and our proof is complete.

We now return to the algebra $\mathfrak{B} = \mathfrak{D}_{\mathfrak{K}} \times \mathfrak{D}_{\mathfrak{K}}$. This is a simple algebra over its center $\mathfrak{K}$ and contains the algebra $\mathfrak{K}[y, y']$. We assume henceforth that $\mathfrak{K}[y, y']$ satisfies the necessary condition of Lemma 4, that is, $\mathfrak{K}(y, y')$ is a field. But clearly the mapping $y \to y_1$, $y' \to y_1^{-1}$ induces an isomorphism of the ring $\mathfrak{K}[y, y']$ onto $\mathfrak{K}[y_1, (y_1')^{-1}]$. Since $\mathfrak{K}[y, y']$ is a field it is a simple algebra and our isomorphism induces an (inner) automorphism of $\mathfrak{B}$ over $\mathfrak{K}$. Thus there exists a regular element d of $\mathfrak{B}$ such that

$$dy_1d^{-1} = y, \qquad dy_1'd^{-1} = (y')^{-1}, \tag{64}$$

that is, such that

$$(dy_J)y(dy_J)^{-1} = y, \qquad (dy_J)y'(dy_J)^{-1} = (y')^{-1}. \tag{65}$$

It follows that

$$(dy_J)^2y - y(dy_J)^2 = (dy_J)^2y' - y'(dy_J)^2 = 0. \tag{66}$$

By our construction of $\mathfrak{A}$ we know that $(dy_J)^2$ is in $\mathfrak{B}$ and commutes with all elements of the maximal subfield $\mathfrak{K}(y, y')$ of $\mathfrak{B}$. It follows that

$$(dy_J)^2 = e = e(y, y') \tag{67}$$

is in the field $\mathfrak{K}(y, y')$. Then

$$[(dy_J)^2]^p = [(dy_J)^2]^2 = e^p = \sigma \tag{68}$$

is in $\mathfrak{K}$. Since $(dy\ )^p\lambda(dy_J)^{-p} = \bar{\lambda}$, for every λ of $\mathfrak{K}$, the element $\sigma = (dy_J)^{2p}$ commutes with $(dy_J)^p$ and *must be in* $\mathfrak{F}$.

Let $\mathfrak{A} = \mathfrak{D} \times \mathfrak{D} \times \mathfrak{M}_2$, so that $\mathfrak{A}$ is a central simple algebra over $\mathfrak{F}$. Then $\mathfrak{A}$ contains $\mathfrak{Q} = (1, u, q_J, uq_J)$ over $\mathfrak{F}$, where $q_J = (dy_J)^p$, $q_Ju = -uq_J$, $q_J^2 = \sigma$. Then $\mathfrak{Q}$ is a quaternion algebra direct factor of $\mathfrak{A}$, and must be isomorphic to $\mathfrak{M}_2$. Thus there exists elements λ and μ in $\mathfrak{K}$ such that $(\lambda + \mu u)(\lambda - \mu u)\sigma = 1$. Put

$$(\lambda + \mu u)(dy_J)^p = fy_J, \tag{69}$$

where f is now in $\mathfrak{B}$, and $(fy_J)^2 = 1$.

Write

$$fx_1f^{-1} = (fy_J)x(fy_J)^{-1} = x^*, \qquad fx_1'f^{-1} = (fy_J)x'(fy_J)^{-1} = x'^*, \quad (70)$$

and see that

$$x^{*p} = x^* + \bar{a}, \qquad x'^{*p} = x'^* + \bar{a}, \qquad x^*x'^* = x'^*x^*. \quad (80)$$

We have also seen that

$$(fy_J)y - y(fy_J) = (fy_J)y' - (y')^{-1}(fy_J) = 0, \quad (81)$$

and so

$$yx^* = (x^* + 1)y, \qquad y'(x')^* = (x'^* - 1)y', \quad (82)$$

and

$$x^*y' - y'x^* = x'^*y - yx'^* = 0. \quad (83)$$

We are now ready to apply the results of Section 5. Since $y(x' - x) = (x' - x)y$ and $y'(x^* - x) = (x^* - x)y'$ we have

$$x^* = x - \phi \quad (84)$$

for an element $\phi = \phi(y, y')$ in $\mathfrak{R}(y, y')$. We also have

$$y'(x'^* + x') - (x'^* + x')y' = y(x'^* + x') - (x'^* + x')y = 0, \quad (85)$$

and so

$$x'^* = \phi' - x', \quad (86)$$

for $\phi' = \phi'(y, y')$ also in $\mathfrak{R}(y, y')$. However, if

$$\psi = \psi(y, y') = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \psi_{ij}y^iy'^j \qquad (\psi_{ij} \text{ in } \mathfrak{R}), \quad (87)$$

we may define

$$\psi^* = (fy_J)\psi(fy_J)^{-1} = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \bar{\psi}_{ij}y^i(y')^{-j}. \quad (88)$$

But then $(fy_J)x^*(fy_J)^{-1} = x = x^* - \phi^* = x - (\phi + \phi^*)$, and

$$(fy_J)x'^*(fy_J)^{-1} = x' = (\phi' - x')^* = \phi'^* - (\phi' - x').$$

Hence

$$\phi^* = -\phi, \qquad \phi'^* = \phi'. \quad (89)$$

We shall finally use the relation $x^*x'^* = x'^*x^*$ of (80). This becomes $(x - \phi)(x' - \phi') = xx' + \phi\phi' - (x\phi' + \phi x') = (x' - \phi')(x - \phi) = x'x + \phi'\phi - (x'\phi + \phi'x)$. Thus $x^*x'^* = x'^*x^*$ if and only if

$$x\phi' - \phi'x = x'\phi - \phi x'. \tag{90}$$

We shall now define two derivations D and D' on the ring $\mathfrak{R}[y, y']$ over $\mathfrak{R}$. We define them by

$$\psi x - x\psi = \psi D, \qquad \psi x' - x'\psi = \psi D'. \tag{91}$$

Then

$$yD = y, \qquad yD' = 0, \qquad y'D = 0, \qquad y'D' = y', \tag{92}$$

and thus, if

$$\psi = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \psi_{ij} y^i (y')^j \qquad (\psi_{ij} \text{ in } \mathfrak{R}), \tag{93}$$

we have

$$\psi D = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \psi_{ij}(iy^i)(y')^j, \qquad \psi D' = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \psi_{ij} j y^i (y')^j. \tag{94}$$

Thus (90) is equivalent to

$$\phi D' = \phi' D. \tag{95}$$

We are now ready to apply the results of Lemma 2. We first consider the algebra $(\mathfrak{H}, y, g\bar{g}) \times \mathfrak{R}(y')$ and see that the fact that $x^{*p} = x^* + \bar{a}$ implies that

$$\bar{a} = a - (\phi^p - \phi_0), \tag{96}$$

where

$$\phi = \sum_{i,j=0}^{p-1} \phi_{ij} y^i y'^j = \sum_{i=0}^{p-1} \phi_i y^i \qquad (\phi_{ij} \text{ in } \mathfrak{R}), \tag{97}$$

and so

$$\phi_i = \sum_{j=0}^{p-1} \phi_j y'^j \qquad [\phi_i \text{ in } \mathfrak{R}(y)]. \tag{98}$$

Note that (96) implies that ϕ_0 is in $\mathfrak{R}$, a result which is also a consequence of (95). We also have $-x'^* = x' - \phi'$ and $(x'^*)^p = (x'^*) + \bar{a}$, so that $(-x'^*)^p = (-x'^*) - \bar{a} = a - [(\phi_0')^p - \phi_0'] + (-x'^*)$, where

$$\phi' = \sum_{i,j=0}^{p-1} \phi'_{ij} y^i y'^j = \sum_{j=0}^{p-1} \phi_j' y'^j, \tag{99}$$

and thus

$$\phi_j' = \sum_{i=0}^{p-1} \phi_{ij}' y^i. \tag{100}$$

Here again we have a relation

$$\bar{a} = -a + \phi'^p - \phi_0'. \tag{101}$$

It follows that

$$2a = (\phi + \phi')^p - (\phi_0 + \phi_0'), \tag{102}$$

where the elements

$$\phi_0 = \phi_{00}, \phi_0' = \phi_{00}' \tag{103}$$

are both in $\mathfrak{K}$.

Write

$$\phi = \phi_{00} + 2\theta, \quad 2\theta = \sum_{i=1}^{p-1} \left(\sum_{j=0}^{p-1} \phi_{ij} y'^j \right) y^i, \tag{104}$$

and

$$\phi' = \phi_{00}' + 2\theta', 2\theta' = \sum_{j=1}^{p-1} \left(\sum_{i=0}^{p-1} \phi_{ij}' y^i \right) (y')^j. \tag{105}$$

Then

$$2a = 2(\theta + \theta')^p + (\phi_{00} + \phi_{00}')^p - (\phi_{00} + \phi_{00}'). \tag{106}$$

The field $\mathfrak{H}$ contains an element $x_2 = x - \frac{1}{2}(\phi_{00} + \phi_{00}')$, and

$$\begin{aligned} x_2^p &= x^p - \tfrac{1}{2}(\phi_{00} + \phi_{00}')^p = x + a - \tfrac{1}{2}(\phi_{00} + \phi_{00}')^p \\ &= x_2 + a - \tfrac{1}{2}[(\phi_{00} + \phi_{00}')^p - (\phi_{00} + \phi_{00}')] = x_2 + (\theta + \theta')^p. \end{aligned}$$

But then we have shown that we can select a canonical generator x of $\mathfrak{H}$ such that $x^p - x = a = (\theta + \theta')^p$. Also $2(\theta D') = \phi D' = \phi' D = 2(\theta' D)$ and so $\theta D' = \theta' D$. It should also be clear that the relations $\phi^* = -\phi$ and $(\phi')^* = \phi'$ imply that $\theta^* = -\theta$, $(\theta')^* = \theta'$. We are now ready to state our main result.

THEOREM 1. *Let $\mathfrak{K}$ be a quadratic extension of a field $\mathfrak{F}$ of characteristic p and $\mathfrak{D}_0 = (\mathfrak{H}, y_S, g)$ be a cyclic division algebra of degree p over $\mathfrak{K}$ such that the field $\mathfrak{N}_0 = \mathfrak{K}(g^{1/p}, \bar{g}^{1/p})$ has degree p^2 over $\mathfrak{K}$ and so is isomorphic to the ring $\mathfrak{N} = \mathfrak{K}[y, y']$, where $y^p = g\bar{g}$, and $(y')^p = g(\bar{g})^{-1}$. Then $\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{K}$ for a*

division algebra $\mathfrak{D}$ *of degree* p *over* $\mathfrak{F}$ *if and only if there exists a canonical generator* x *of the cyclic field* $\mathfrak{H}$ *over* $\mathfrak{K}$ *such that*

$$x^p - x = a = (\theta + \theta')^p, \tag{107}$$

for elements

$$\theta = \sum_{i=1}^{p-1}\sum_{j=0}^{p-1} \theta_{ij} y^i (y')^j, \theta' = \sum_{j=1}^{p-1}\sum_{i=0}^{p} \theta'_{ij} y^i (y')^j \qquad (\theta_{ij}, \theta'_{ij} \text{ in } \mathfrak{K}) \tag{108}$$

in $\mathfrak{N}$ *such that*

$$\theta D' = \theta' D, \qquad \theta^* = -\theta, \qquad \theta'^* = \theta'. \tag{109}$$

For we have actually shown that the condition $\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{K}$ implies the existence of a generator x of $\mathfrak{H}$ over $\mathfrak{K}$ satisfying (107), (108), and (109), and that the implication is a direct consequence of the hypothesis that $\mathfrak{D}_1 \times \mathfrak{D}_2 = (\mathfrak{H}, y, g\bar{g}) \times (\mathfrak{H}', y', g/\bar{g})$ *has an automorphism* $d \to d^*$ *over* $\mathfrak{F}$ *induced by the mappings* $x \to x^*$, $y \to y^* = y$, $x' \to x'^*$, $y' \to y'^* = (y')^{-1}$, $\lambda \to \lambda^* = \bar{\lambda}$ *for every* λ *of* $\mathfrak{K}$. Conversely, the conditions (107), (108), and (109) imply that, if we define $x^* = x - 2\theta$, $x'^* = 2\theta' - x$, $y^* = y$, $y'^* = (y')^{-1}$, $\lambda^* = \bar{\lambda}$, then $x^{*p} = x^* + \bar{a}$, $(x'^*)^p = x'^* + \bar{a}$, $y^* x^* - (x^* + 1)y^* = y'^* x'^* - (x'^* + 1)y'^* = y^* x'^* - x'^* y^* = y'^* x^* - x^* y'^* = x^* x'^* - x'^* x^* = 0$. But then the mapping $d \to d^*$, induced by our definitions, is an automorphism of $\mathfrak{D}_1 \times \mathfrak{D}_2$ over $\mathfrak{F}$. It clearly has period two and induces the automorphism $\lambda \to \bar{\lambda}$ of $\mathfrak{K}$ over $\mathfrak{F}$. Then $\mathfrak{K} = \mathfrak{F}(u)$, where $\bar{u} = -u$, and every element k of $\mathfrak{D}_1 \times \mathfrak{D}_2$ has the form $k = k_1 + k_2 u$ for $k_1 = \frac{1}{2}(k + k^*) = k_1^*$ and $k_2 = \frac{1}{2}(d - d^*)u^{-1} = k_2^*$. Then the set $\mathfrak{B}$, of all elements $k = k^*$ of $\mathfrak{D}_1 \times \mathfrak{D}_2$, is a central simple algebra of degree p^2 over $\mathfrak{F}$ since, in fact, $\mathfrak{D}_1 \times \mathfrak{D}_2 = \mathfrak{B} \times \mathfrak{K}$. Since $\mathfrak{D}_1 \times \mathfrak{D}_2 = \mathfrak{D}_0^2 \times \mathfrak{M}_p$ we mu t have $\mathfrak{B} = \mathfrak{D}_3 \times \mathfrak{M}_p$ where $\mathfrak{D}_3$ is a central division algebra of degree p over $\mathfrak{F}$, $\mathfrak{D}_3 \times \mathfrak{K}$ is isomorphic to $\mathfrak{D}_0^2$ and so $\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{K}$, where $\mathfrak{D}^2$ is isomorphic to $\mathfrak{D}_3$, $\mathfrak{D}$ is a central division algebra over $\mathfrak{F}$ as desired.

The algebra $\mathfrak{B}$ can be computed explicitly. Indeed, let

$$z = (x - \theta), \qquad w = x' - \theta'. \tag{110}$$

The fact that $\theta D' = \theta' D$ then implies that $zw = wz$. It follows immediately that

$$\mathfrak{D}_1 \times \mathfrak{D}_2 = (\mathfrak{Z}, y, g\bar{g}) \times (\mathfrak{W}, y', g/\bar{g}), \tag{111}$$

where $\mathfrak{Z} = \mathfrak{F}(z)$ and $\mathfrak{W} = \mathfrak{K}(w)$, $yz = (z + 1)g$, $yw = wy$, $y'z = zy'$, $y'w = (w + 1)y'$. Moreover the result in (47) implies that $z^p - z = a_1 = a - \theta^p = a - \frac{1}{2}(a - \bar{a}) = \frac{1}{2}(a + \bar{a})$, $w^p - w = a_2 = a - (\theta')^p = a - \frac{1}{2}(a + \bar{a}) = \frac{1}{2}(a + \bar{a})$. The algebra $(\mathfrak{Z}, y, g\bar{g})$ is cyclic over $\mathfrak{F}$. We put

$$w_1 = w(y' + y'^{-1})[y' - (y')^{-1}]^{-1}. \tag{112}$$

In the algebra $(\mathfrak{W}, y', g/\bar{g})$ the norm of w is $\frac{1}{2}(a - \bar{a})$, and the norm of $(y' + y'^{-1})[y' - (y')^{-1}]$ is its pth power $[g(\bar{g})^{-1} + \bar{g}g^{-1}][g(\bar{g})^{-1} - \bar{g}g^{-1}]^{-1} = (g^2 + g^{-2})(g^2 - \bar{g}^2)^{-1}(g^2 - \bar{g}^2)^{-1}$. Thus the norm of w_1 is an element $a_3 = \frac{1}{2}(a - \bar{a})(g^2 + \bar{g}^2)(g^2 - \bar{g}^2)^{-1}$ and is in $\mathfrak{F}$. Then it is easy to see that, if $y_1 = y' + y'^{-1}$, we have $y_1 w_1 = (w_1 + 1)y_1$ and so ${w_1}^p = w_1 + a_3$, where a_3 is in F, $g_1 = {y_1}^p = (g^2 + \bar{g}^2)(g\bar{g})^{-1}$ is in $\mathfrak{F}$, and so $\mathfrak{D}_1 \times \mathfrak{D}_2 = (3, y, g\bar{g}) \times (\mathfrak{W}_1, y_1, g_1) \times \mathfrak{R}$. But $\mathfrak{D}_1 \times \mathfrak{D}_2 = {\mathfrak{D}_0}^2 \times \mathfrak{M}_p$. It follows that $(3, y, g\bar{g}) \times (\mathfrak{W}_1, y_1, g_1) = \mathfrak{D}_1 \times \mathfrak{M}_p$, where $\mathfrak{D}_1$ is a division algebra over $\mathfrak{F}$, such that $\mathfrak{R} \times \mathfrak{D}_1$ is isomorphic over $\mathfrak{R}$ to ${\mathfrak{D}_0}^2$. But then $\mathfrak{D}_1 = \mathfrak{D}^2$ for a division algebra $\mathfrak{D}$ of degree p over its center $\mathfrak{F}$, and $\mathfrak{D}_0$ is isomorphic to $\mathfrak{D} \times \mathfrak{R}$ as desired.

7. Change of Generators

Let us proceed to the derivation of an elementary property regarding a change of the generators of a cyclic algebra $\mathfrak{E} = (\mathfrak{H}, y, g)$ over $\mathfrak{R}$, where $\mathfrak{E}$ is a division algebra, $\mathfrak{H} = \mathfrak{R}(x)$, $x^p - x = a$ in $\mathfrak{R}$, $yx = (x + 1)y$, $y^p = g$. Then $\mathfrak{R}[y]$ is a field and, if

$$\phi = \phi(y) = \phi_0 + \phi_1 y + \cdots + \phi_{p-1} y^{p-1} \tag{113}$$

for ϕ_i in $\mathfrak{R}$ and $\phi \neq \phi_0$, we have already seen that $\phi x = x\phi + \phi D$ where $\phi D = \sum_{i=0}^{p-1} i\phi_i y^i$. Then ϕD is a nonsingular element of $\mathfrak{R}(y)$ and $\mathfrak{R}(\phi) = \mathfrak{R}(y$ is a field of degree p over $\mathfrak{R}$.

We now let

$$x_0 = x[\phi(\phi D)^{-1}], \tag{114}$$

and have

$$\phi^p = g_0 = \sum_{i=0}^{p-1} \phi_i{}^p g^i. \tag{115}$$

Then $\phi x_0 = \phi x \phi(\phi D)^{-1} = (x\phi + \phi D)\phi(\phi D)^{-1} = [x\phi(\phi D)^{-1} + 1]\phi = (x_0 + 1)\phi$. We also know that the algebra $\mathfrak{E}$ has a multiplicative norm form $N(d)$ on $\mathfrak{E}$ to $\mathfrak{R}$, $N(x) = a$, $N(\phi) = \phi^p$, $N(\phi D) = (\phi D)^p$, so that

$$x_0{}^p - x_0 = a_0 = a[\phi^p(\phi D)^{-p}]. \tag{116}$$

We have derived the following result.

Lemma 5. *Let $\mathfrak{E} = (\mathfrak{H}, y, g)$ where $\mathfrak{H}$ and y are as above, and ϕ be any element of the field $\mathfrak{R}(y)$ not in $\mathfrak{R}$. Then $\mathfrak{E} = (\mathfrak{H}_0, \phi, g_0)$, where $g_0 = \phi^p$ in $\mathfrak{R}$, $\mathfrak{H}_0 = \mathfrak{R}(x_0)$ for $x_0{}^p - x = a_0 = a[\phi^p(\phi D)^{-1p}]$.*

8. A Special Case

We let $\mathfrak{F}_p$ be the field of p elements, ξ and η be independent indeterminates over $\mathfrak{F}_p$ and take

$$\mathfrak{K} = \mathfrak{F}_p(\xi, \eta), \qquad \mathfrak{F} = \mathfrak{F}_p(\xi, \eta^2), \qquad g = \xi + \eta. \tag{117}$$

Then $\mathfrak{K} = \mathfrak{F}(u)$ with $u = \eta$. We now construct the cyclic algebra $\mathfrak{D}_0 = (\mathfrak{H}, y_S, g)$, where

$$\mathfrak{H} = \mathfrak{K}(x), \qquad x^p - x = a, \qquad yx = (x+1)y, \qquad y^p = g. \tag{118}$$

Take

$$\theta = \eta y, \qquad \theta' = y' + (y')^{-1}, \qquad y^p = g\bar{g}, \qquad y'^p = g(\bar{g})^{-1}, \tag{119}$$

so that $\theta^* = -\theta$, $(\theta')^* = \theta'$. Then

$$\theta^p = \eta^p g\bar{g}, \qquad \theta'^p = g(\bar{g}^{-1}) + \bar{g}(g^{-1}), \tag{120}$$

and we define

$$a = (\theta + \theta')^p = (g\bar{g})^{-1}[\eta^p(g\bar{g})^2 + g^2 + \bar{g}^2]. \tag{121}$$

Since $\theta D' = \theta' D = 0$ we apply Theorem 1 to see that, if $\mathfrak{K}[g^{1/p}, \bar{g}^{1/p}]$ is a field of degree p^2 over $\mathfrak{K}$, then $\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{K}$ for a division algebra $\mathfrak{D}$ of degree p over $\mathfrak{F}$. We first derive the following result.

Lemma 6. *The ring $\mathfrak{K}[y, y']$ is a field of degree p^2 over $\mathfrak{K}$.*

Our study will lean heavily on degree considerations and the fact that the polynomial rings $\mathfrak{E} = \mathfrak{F}_p[\xi, \eta]$ and $\mathfrak{E}' = \mathfrak{F}_p[\xi, \eta^2]$ are *unique factorization integral domains*. Note that g, $\bar{g}$, η are irreducible polynomials of $\mathfrak{E}$ since they are all linear in η. Also $g\bar{g} = \xi^2 - \eta^2$ and $g^2 + \bar{g}^2 = 2(\xi^2 + \eta^2)$ are irreducible polynomials of $\mathfrak{E}'$.

We first observe that $\mathfrak{K}(g^{1/p})$ is a field of degree p over $\mathfrak{K}$. For otherwise $g = \beta^p$ for β in $\mathfrak{K}$. We may then write $\beta = \gamma\delta^{-1}$ for γ and δ in $\mathfrak{E}$, $g\delta^p = (\xi+\eta)_i\delta^p = \gamma^p$. The degree in η of every term of γ^p is divisible by p, and the degree in η of $(\xi + \eta)\delta^p$ is the degree in η of $\eta\delta^p$ and has the form $p\alpha + 1$. This is impossible and so $\mathfrak{K}_1 = \mathfrak{K}(g^{1/p})$ has degree p over $\mathfrak{K}$. If $\mathfrak{K}_1(\bar{g}^{1/p})$ does not have degree p over $\mathfrak{K}_1$ then $\bar{g}^{1/p}$ is in $\mathfrak{K}$, $\bar{g} = m^p$ for $m = \beta_0 + \beta_1 g^{1/p} + \cdots + \beta_{p-1}(g^{1/p})^{p-1}$ in $\mathfrak{K}_1$, that is, for the β_i in $\mathfrak{K}$. We then write $\beta_i = \gamma_i\delta^{-1}$ where the polynomials $\gamma_0, \gamma_1, \ldots, \gamma_{p-1}$, δ do not have a nonconstant polynomial common factor. But then

$$\bar{g}\delta^p = (\delta m)^p = \gamma_0{}^p + \gamma_1{}^p g + \cdots + \gamma_{p-1}^p g^{p-1}. \tag{122}$$

The ring

$$\mathfrak{E} = \mathfrak{F}_p[\xi, \eta] = \mathfrak{F}_p[\xi, g],\ \xi - \eta = \bar{g} = 2\xi - g \tag{123}$$

and we may write

$$\delta = \sum_{j=0}^{r} \delta_j g^j, \qquad \gamma_i = \sum_{j=0}^{s} \gamma_{ij} g^j, \tag{124}$$

for δ_j and γ_{ij} in $\mathfrak{F}_p[\xi]$ and $\delta_r \neq 0$. The constant terms relative to g in

$$(2\xi - g)\delta^p + \gamma_0{}^p + \gamma_1{}^p g + \cdots + \gamma_{p-1}^p g^{p-1} \tag{125}$$

yield the equation

$$2\xi\delta_0{}^p = \gamma_{00}^p . \tag{126}$$

Degree considerations imply that $\delta_0 = \gamma_{00} = 0$, δ has g as a factor, $\delta = \delta' g$, $\gamma_0 = \gamma_0' g$ and we obtain

$$(2\xi - g)g^p\delta'^p = (\gamma_0')^p g^p + \gamma_1{}^p g + \cdots + \gamma_{p-1}^p g^{p-1}. \tag{127}$$

If $\gamma_1, \ldots, \gamma_t$ all have g as a factor we see that g^p divides the left member of (119) and $\gamma_0{}^p + \gamma_1{}^p g + \cdots + \gamma_t{}^p g^t$ and so divides $\gamma_{t+1}^p g^t + \cdots + \gamma_{p-1}^p g^{p-1}$. Then γ_{t+1}^p is divisible by g and so is γ_{t+1}. This completes an inductive proof of the fact that $\gamma_0, \ldots, \gamma_{p-1}$ are all divisible by g contrary to our hypothesis. Thus $\mathfrak{R}_1(g^{1/p}) = \mathfrak{R}(g^{1/p}, \bar{g}^{1/p})$ has degree p over $\mathfrak{R}_1$, degree p^2 over $\mathfrak{R}$, and our proof of the lemma is complete.

9. The Cyclicity Condition

Lemma 2 states that our algebra $\mathfrak{D}_0 = (\mathfrak{H}, y_S, g)$ is split by a field $\mathfrak{R}_0 = \mathfrak{R}(\epsilon^{1/p})$ if and only if

$$a = \lambda^p - \lambda + \sum_{i=1}^{p-1} \phi_i{}^p g^i \tag{128}$$

for $\lambda, \phi_1, \ldots, \phi_{p-1}$ in $\mathfrak{R}_0$. Evidently $a, g, \phi_i{}^p, \lambda^p$ are all in $\mathfrak{R}$. Hence λ must be in $\mathfrak{R}$. But, if we select a so that $\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{R}$, then $\mathfrak{D}$ *is cyclic if and only if there exists an* ϵ *in* $\mathfrak{F}$ *such that* $\mathfrak{R}_0 = \mathfrak{R}(\epsilon^{1/p})$ *splits* $\mathfrak{D}_0$. Moreover we may write

$$a = \lambda^p - \lambda + \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \phi_{ij}^p g^i \epsilon^j, \tag{129}$$

where λ and the ϕ_{ij} are all in $\mathfrak{R}$.

It is clear that, in our special case, we may always select ϵ in $\mathfrak{E} = \mathfrak{F}_p[\xi, \eta]$. We may also write

$$\lambda = \mu\nu^{-1} \tag{130}$$

for polynomials μ and ν of $\mathfrak{E}$ such that the elements $\nu\phi_{ij} = \theta_{ij}$ are in $\mathfrak{E}$, and the polynomials μ, ν, θ_{ij} *do not all have a factor in common.* Thus (129) becomes

$$a\nu^p = \mu^p - \mu\nu^{p-1} + \sum_{i=1}^{p-1}\sum_{j=0}^{p-1} \theta_{ij}^p g^i \epsilon^j. \tag{131}$$

We now propose to show that $\mathfrak{K}_0 = \mathfrak{K}(\xi^{1/p})$ does not split $\mathfrak{D}_0$. For proof we observe first that

$$\bar{g}^{1/p} = 2\xi^{1/p} - g^{1/p}. \tag{132}$$

We define

$$x_0 = x(y_S - 2\xi^{1/p})y_S^{-1}, \qquad y_0 = 2\xi^{1/p} - y_S, \tag{133}$$

so that $y_0{}^p = 2\xi - g = \bar{g}$;

$$x_0{}^p - x_0 = a_0 = -a\bar{g}g^{-1} = -g^{-2}[\eta^p(g\bar{g})^2 + g^2 + \bar{g}^2]. \tag{134}$$

Since $y_0 D = -y_S$ we know that $x_0 = xy_0(y_0 D)^{-1}$ and it follows from Lemma 5 that $\mathfrak{D}_0 \times \mathfrak{K}_0 = (\mathfrak{H}_0, y_0, \bar{g})$, where $\mathfrak{H}_0 = \mathfrak{K}_0(x_0)$. We use this new generation of $\mathfrak{D} \times \mathfrak{K}_0$ to see that $\mathfrak{D}$ is split by $\mathfrak{K}_0$ if and only if

$$[\eta^p(g\bar{g})^2 + g^2 + \bar{g}^2]\nu^p + \left[(\mu^p - \mu\nu^{p-1}) + \sum_{i=1}^{p-1}\sum_{j=0}^{p-1} \theta_{ij}^p \xi^j \bar{g}^i\right] g^2 = 0 \tag{135}$$

for ν, μ, θ_{ij} in $\mathfrak{E}$ and not all having a polynomial nonconstant factor in common. But (135) implies that $\bar{g}$ divides

$$g^2(\nu^p + \mu^p - \mu\nu^{p-1}) \tag{136}$$

and hence divides $\nu^p + \mu^p - \mu\nu^{p-1}$. Let us now use the fact that $\mathfrak{E} = \mathfrak{F}_p[\xi, \bar{g}]$ write $\mu = \sum_{i=0}^{q} \mu_i \bar{g}^i$, $\nu = \sum_{i=0}^{r} \nu_i \bar{g}^i$ for μ_i and ν_i in $\mathfrak{F}_p[\xi]$. Then our divisibility property implies that

$$\mu_0{}^p - \mu_0\nu_0^{p-1} + \nu_0{}^p = 0. \tag{137}$$

We now write $\mu_0 = \sum_{j=0}^{s} \mu_{0j}\xi^j$, $\nu_0 = \sum_{j=0}^{t} \nu_{0j}\xi^j$ for μ_{0j} and ν_{0j} in $\mathfrak{F}_p$. In particular we clearly see that (137) implies that $\mu_{00}^p - \mu_{00}v_{00}^{p-1} + v_{00}^p = 0 = \mu_{00} - \mu_{00}\nu_{00}^{p-1} + v_{00}^p$. If $\nu_{00} \neq 0$, then $\nu_{00}^{p-1} = 1$ and so $\mu_{00} - \mu_{00} + \nu_{00} = \nu_{00} = 0$, a contradiction. Hence $\nu_{00} = 0 = \mu_{00}$. Then $\mu_0 = \xi\mu_0'$ and $\nu_0 = \xi\nu_0'$ and

(137) becomes $(\mu_0'^p - \mu_0'\nu_0'^{p-1} + \nu_0'^p)\xi^p = 0$ and we are led to an equation of the same form as (137) but with degrees reduced by one. This clearly implies that $\mu_0 = \nu_0 = 0$, and so $\bar{g}$ divides both μ and ν. This yields $[\eta^p(g\bar{g})^2 + g^2 + \bar{g}^2]\nu^p + \mu^p - \mu\nu^{p-1} \equiv 0 \pmod{\bar{g}^p}$ and so

$$\sum_{i=1}^{p-1}\sum_{j=0}^{p-1} \theta_{ij}^p \xi^j \bar{g}^i \equiv 0 \pmod{\bar{g}^p}. \tag{138}$$

We have already used the fact that

$$\mathfrak{E} = \mathfrak{F}_p[\xi, \eta] = \mathfrak{F}_p[\xi, \bar{g}] = \mathfrak{F}_p[\xi, g], \tag{139}$$

a consequence of the fact that $g = \xi + \eta$. We now derive the following result.

LEMMA 7. *Let $\rho = \rho_0^p + \rho_1^p\xi + \cdots + \rho_{p-1}^p\xi^{p-1}$ for polynomials ρ_i in $\mathfrak{E}$. Then $\bar{g}$ divides ρ if and only if $\bar{g}$ divides $\rho_0, \rho_1, \ldots, \rho_{p-1}$.*

For we write $\rho_i = \sum_{j=0}^{s} \rho_{ij}\bar{g}^j \equiv \rho_{i0} \pmod{\bar{g}}$, where the ρ_{ij} are all in $\mathfrak{F}_p[\xi]$. Then $\rho \equiv 0 \pmod{\bar{g}}$ if and only if

$$\sigma = \rho_{00}^p + \rho_{10}^p\xi + \cdots + \rho_{p-1}^p\xi^{p-1} = 0. \tag{140}$$

The degree in ξ *of every term* of $\rho_{i0}^p\xi^i$ has the form $ps_i + i$ where $0 \leqslant i < p$, and so $\sigma = 0$ only if every $\rho_{i0} = 0$, $\bar{g}$ divides every ρ_i.

As a consequence we have the following result.

LEMMA 8. *Let $\rho = \rho_0^p + \rho_1^p g + \cdots + \rho_{p-1}^p g^{p-1} \equiv 0 \pmod{\bar{g}}$, for ρ_i in $\mathfrak{E}$. Then $\bar{g}$ divides every ρ_i. If $\rho = \rho_0^p + \rho_1^p\bar{g} + \cdots + \rho_{p-1}^p\bar{g}^{p-1} \equiv 0 \pmod{g}$ for ρ_i in $\mathfrak{E}$. Then g divides every ρ_i.*

For we observe that $g = 2\xi - \bar{g}$ and so $g^i \equiv (2\xi)^i \pmod{\bar{g}}$ and $\rho \equiv \sum_{i=0}^{p-1}(2^i\rho_i)^p\xi^i \pmod{\bar{g}}$ and our result follows from Lemma 7. The second result is obtained by taking conjugates.

We are now ready to derive our contradiction. We observe that (138) implies that $\sum_{j=0}^{p-1}\theta_{ij}^p\xi^j \equiv 0 \pmod{\bar{g}}$. By Lemma 7 every $\theta_{ij} \equiv 0 \pmod{\bar{g}}$ and $\sum_{j=0}^{p-1}\theta_{ij}^p\xi^j \equiv 0 \pmod{\bar{g}^p}$. If every $\theta_{ij} \equiv 0 \pmod{\bar{g}}$ for $i = 1, \ldots, s$ and $j = 0, 1, \ldots, p-1$, then $\sum_{i=1}^{s}\sum_{j=0}^{p-1}\theta_{ij}^p\bar{g}^{ip}\xi^{jp} \equiv 0 \pmod{\bar{g}^p}$, and if $1 \leqslant s < p-1$ we obtain $\sum_{j=0}^{p-1}\theta_{s+1,j}^p\xi^j \equiv 0 \pmod{\bar{g}}$, and so every $\theta_{s+1.j} \equiv 0 \pmod{\bar{g}}$. This completes an inductive proof of the fact that every $\theta_{ij} \equiv 0 \pmod{\bar{g}}$. But then μ, ν, and all θ_{ij} have $\bar{g}$ as a factor contrary to hypothesis.

We have derived the following result.

THEOREM 2. *Let $a = [\eta^p(g\bar{g})^2 + g^2 + \bar{g}^2](g\bar{g})^{-1}$ and $\mathfrak{D}_0 = (\mathfrak{H}, y, g)$ over $\mathfrak{K}$, where $\mathfrak{H} = \mathfrak{K}(x)$, $x^p - x = a$. Then $\mathfrak{D}_0$ is a division algebra, and $\mathfrak{K}_0 = \mathfrak{K}(\xi^{1/p})$ does not split $\mathfrak{D}_0$.*

10. The Non-Normality of $\mathfrak{H}$

We know already that if $\mathfrak{H}$ is a normal field over $\mathfrak{F}$, the algebra $\mathfrak{D}$ defined by $\mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{K} = (\mathfrak{H}, y_S, g)$ is cyclic. Let us then show that $\mathfrak{H}$ is not normal over $\mathfrak{F}$ in our special case.

Let us show first that $\mathfrak{D}_0$ contains no element x_1 such that $x_1^p - x_1 = a_1 = -\bar{a}_1$ and $y_S x_1 = (x_1 + 1)y_S$. We have already seen that $x_1 = x - \psi$ for ψ in $\mathfrak{K}[y_S]$, and that

$$a_1 = [\eta^p(g\bar{g})^2 + g^2 + \bar{g}^2](g\bar{g})^{-1} - (\lambda^p - \lambda) - \sum_{i=1}^{p-1} \psi_i^p g^i. \tag{141}$$

Then $a_1 = -\bar{a}_1$ if and only if

$$2(g^2 + \bar{g}^2)(g\bar{g})^{-1} = (\lambda + \bar{\lambda})^p - (\lambda + \bar{\lambda}) + \sum_{i=1}^{p-1} (\psi_i^p g^i + \bar{\psi}_i^p \bar{g}^i). \tag{142}$$

The element $\frac{1}{2}(\lambda + \bar{\lambda})$ is in $\mathfrak{F}$ and we can write

$$\tfrac{1}{2}(\lambda + \bar{\lambda}) = \mu\nu^{-1}, \qquad \tfrac{1}{2}(\psi_i \nu) = \theta_i, \tag{143}$$

for elements μ and ν in $\mathfrak{F}_p[\xi, \eta^2]$, θ_i in $\mathfrak{F}_p[\xi, \eta]$. Indeed, $\psi_i = \psi_i' \psi_0^{-1}$ for ψ_i' and ψ in $\mathfrak{F}_p[\xi, \eta]$, $(\psi_0\bar{\psi}_0)^p(\psi_i^p g^i + \bar{\psi}_i^p \bar{g}^i) = (\bar{\psi}_0\psi_i')^p g^i + (\psi_0\bar{\psi}_i')^p \bar{g}^i$ has coefficients in $\mathfrak{F}_p[\xi, \eta]$. Thus ν can be chosen to be divisible by $\psi_0\bar{\psi}_0$ and θ_i is in $\mathfrak{F}_p[\xi, \eta]$. We may clearly select μ and ν so that $\mu, \nu, \theta_1, \ldots, \theta_{p-1}$ have no nonconstant factor in common. Thus we obtain

$$(g^2 + \bar{g}^2)\nu^p = \left[(\mu^p - \mu\nu^{p-1}) + \sum_{i=1}^{p-1} (\theta_i^p g^i + \bar{\theta}_i^p \bar{g}^i)\right] g\bar{g}. \tag{144}$$

It follows immediately that $g\bar{g}$ divides ν^p and hence ν, $\nu = \nu' g\bar{g}$ for ν' in $\mathfrak{F}_p[\xi, \eta^2]$. Thus

$$(g^2 + \bar{g}^2)\nu'^p(g\bar{g})^{p-1} = [\mu^p - \mu(\nu')^{p-1}(g\bar{g})^{p-1}] + \sum_{i=1}^{p-1} (\theta_i^p g^i + \bar{\theta}_i^p \bar{g}^i). \tag{145}$$

But then

$$\mu^p + \sum_{i=1}^{p-1} \bar{\theta}_i^p \bar{g}^i \equiv 0 \pmod{g}. \tag{146}$$

By Lemma 8 we see that g divides $\mu, \bar{\theta}_1, \ldots, \bar{\theta}_{p-1}$. Similarly, $\bar{g}$ divides $\mu, \theta_1, \ldots, \theta_{p-1}$ and we write $\mu = \mu' g\bar{g}$, $\theta_i = \theta_i' \bar{g}$ for μ' in $\mathfrak{F}_p[\xi, \eta^2]$ and θ_i' in $\mathfrak{F}_p[\xi, \eta]$. Then (145) becomes

$$(g^2 + \bar{g}^2)\nu'^p(g\bar{g})^{p-1} = (\mu'^p - \mu'\nu'^{p-1})(g\bar{g})^p + \sum_{i=1}^{p-1} (\theta_i'^p g^i \bar{g}^p + \bar{\theta}_i'^p \bar{g}^i g^p). \tag{147}$$

Then $(g\bar{g})^{p-1}$ divides $\sum_{i=1}^{p-1} (\theta_i'^p g^i \bar{g}^p + \bar{\theta}_i'^p \bar{g}^i g^p)$ and it follows that g^{p-1} divides $\sum_{i=1}^{p-2} \theta_i'^p g^i$. The fact that g^{p-1} divides $\sum_{i=1}^{p-2} \bar{\theta}_i'^p g^i$ then implies easily that g divides θ_i' for $i = 1,..., p-2$ and so we write $\theta_i' = \theta_i'' g$ for θ_i' in $\mathfrak{F}_p[\xi, \eta]$ and $i = 1,..., p-2$. Then $\bar{\theta}_i' = \bar{\theta}_i'' \bar{g}$ for $i = 1,..., p-2$. But then $\bar{g}^{p+1}\nu'^p - (\theta'_{p-1})^p \bar{g}^p$ is divisible by g and so is $\bar{g}\nu'^p - \theta'^p_{p-1}$. By Lemma 8 we know that θ_{p-1} and ν' are both divisible by g. This contradicts our hypothesis and our proof is complete. We state this result as follows.

THEOREM 3. *Let $\mathfrak{D}_0$ be the algebra $(\mathfrak{H}, y_S, g)$ of our special case. Then there exists no element x_1 in $\mathfrak{D}_0$ such that $y_S x_1 = (x_1 + 1)y_S$, $x_1^p - x_1 = a_1 = -\bar{a}_1$. In particular, there is no element x_1 in $\mathfrak{H}$ with this property.*

There remains the case where $\bar{a}_1 = a_1$. In this case we are able only to show that $\mathfrak{H}$ contains no such element x_1. For we can restrict our attention to the case that $x_1 = x - \lambda$ for λ in $\mathfrak{K}$, $x_1^p - x_1 = x^p - \lambda^p - (x - \lambda) = a_1 = a - (\lambda^p - \lambda)$. Suppose then that

$$[\eta^p(g\bar{g})^2 + g^2 + \bar{g}^2](g\bar{g})^{-1} - (\lambda^p - \lambda) = [-\eta^p(g\bar{g})^2 + g^2 + \bar{g}^2](g\bar{g})^{-1} - (\bar{\lambda}^p - \bar{\lambda}), \tag{148}$$

a result equivalent to

$$2\eta^p(g\bar{g}) = (\lambda - \bar{\lambda})^p - (\lambda - \bar{\lambda}). \tag{149}$$

We may now write

$$\lambda - \bar{\lambda} = 2\eta\mu\nu^{-1} \tag{150}$$

for μ and ν in $\mathfrak{F}_p[\xi, \eta^2]$ and *having no nonconstant factor in common*. Thus we have

$$\eta^p \nu^p g\bar{g} = (\eta\mu)^p - \eta\mu\nu^{p-1}.$$

If ν has a prime factor distinct from η this factor divides $(\eta\mu)^p$ and must divide μ contrary to hypothesis. Hence $\nu = k\eta^r$ for $k \neq 0$ in $\mathfrak{F}_p$ and $r \geqslant 0$. If $r = 0$ then $\eta^p k g\bar{g} = \eta^p\mu^p - \eta\mu$. The degree in η of the left member is $p + 2$ and the degree in η of the right member is $p(s + 1)$ where s is the degree of μ. This is impossible. If $r = 1$ then $g\bar{g}\eta^p k = \mu^p - \mu$. Our degree consideration then implies that this is impossible. Hence $r > 1$ and $kg\bar{g}\beta\eta^{rp} = \mu^p - \mu\eta^{r(p-1)+1-p}$ where $r(p-1) - (p-1) = (r-1)(p-1) > 0$. But then η divides μ and we obtain a contradiction. We have derived the following result.

THEOREM 4. *In our special case the field $\mathfrak{H}$ is not normal over $\mathfrak{F}$.*

Let us observe that if $\mathfrak{D}_0$ contains an element x_1 such that $y_S x_1 = (x_1 + 1)y_S$ and $x_1^p - x_1 = a_1 = \bar{a}_1$ then $\mathfrak{H}_1 = \mathfrak{K}(x_1) = \mathfrak{F}(x_1) \times \mathfrak{K}$. It follows imme-

diately that $\mathfrak{D}_0 = (\mathfrak{H}_1, y_T, \bar{g})$, $\mathfrak{D}_0^2 = (\mathfrak{H}_1, y, g\bar{g})$. Thus $\mathfrak{D}_0$ contains an element x_1 of our type only if $\mathfrak{R}((g\bar{g})^{1/p})$ splits $\mathfrak{D}_0^2$. But we have already seen that $\mathfrak{D}_0 \times \mathfrak{D}_0 = (\mathfrak{Z}, y, g\bar{g}) \times (\mathfrak{W}, y', g/\bar{g})$ and so $\mathfrak{R}((g\bar{g})^{1/p})$ splits $\mathfrak{D}_0$ if and only if $\mathfrak{R}((g\bar{g})^{1/p})$ splits $(\mathfrak{W}, y', g/\bar{g})$. Since one of the cases in a possible proof that our algebra D is not cyclic is a study of the case where $\epsilon = g\bar{g}$, it will be a part of a program hopefully designed to prove that property for $n = 5$.

Printed in Belgium.